

REMARKS

Claims 1-11 are pending in the application.

Claims 1, 3 and 5-11 are rejected under 35 U.S.C. 102(b) as being anticipated by Choo (U.S. Patent No. 6,981,140).

Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Choo in view of Iitsuka et al. (U.S. Patent No. 6,463,151).

Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Choo in view of Albrecht et al. (U.S. Patent No. 6,510,521).

The claims are amended, claim 10 is cancelled without disclaimer or prejudice, and, thus, the pending claims remain for reconsideration, which is requested. No new matter has been added.

The independent claims are 1, 5, 6, 8, 9, and 11, which are rejected as being anticipated by Choo. In the Office Action, the Examiner asserts that Choo (US 6,981,140) teaches all the elements recited in Claim 1 of the present application.

The Office Action relies upon FIGs. 5-6 and column 10, line 38 to column 11, line 25. However, the configuration Choo's FIGS. 5 and 6 differ from the language of claims. For example, the language of claim 1 provides "an encryption data transmitting portion that transmits encryption data that is necessary for encrypting the information in accordance with the encryption rule over the network to the information management system." Choo does not expressly discuss transmission of its security policy 605 from the IPSec stack 510 to the network protocol stack in the first OS memory area 502, but expressly discusses that the packet to be transmitted enters the redirector layer 508 in first OS memory area 502 and is redirected via port 509 to the IPSec stack 510 in the second user memory area 503, at which time the IPSec stack 510 consults its security database to determine whether the data packet received from the user process 600 is to be encrypted prior to transmission across the network (see column 13, lines 5-26). Thus, Choo is silent on any "transmits encryption data that is necessary for encrypting the information in accordance with the encryption rule over the network to the information management system," because no such transmission is mentioned in Choo. Further, Choo fails to expressly or inherently disclose claimed "***over the network***" configuration as claimed.

Further, there is no evidence that Choo's IPsec stack 510 inherently or necessarily requires transmitting a security policy 605 to the network protocol stack in the first OS memory area 502. Thus, a prima facie case of anticipation cannot be established, because Choo fails to disclose expressly or inherently each and every element of the claim 1, namely "transmits encryption data that is necessary for encrypting the information in accordance with the encryption rule over the network to the information management system."

Further, the language of claims provides "a warning portion that warns the information management system over the network, if the monitoring portion has determined that the information is not encrypted in accordance with the encryption rule." The Office Action relies upon column 11, lines 3-25 and asserts that Choo's use of IKE 604 is same as the claimed "warning portion." However, the difference between Choo and the present invention are as follows. The technology disclosed by Choo is directed to IP Security Protocol (IPsec). According to the technology disclosed by Choo, an encryption scheme is selected based on a negotiation procedure that is performed before initiating communication between two parties, if IPsec stack 510 detects that it has not received a security association (see col. 11, line 10-13).

In contrast, the language of claim 1 provides that an encryption rule is defined for each secret level and those encryption rules are stored in the encryption rule storing portion. Then, information is encrypted based on the encryption rule corresponding to a secret level for the classification of the information. And the monitoring section monitors whether such encryption has taken place, and if not warns the information management system. In other words, Choo initiates Internet Key Exchange (IKE) 604 when no security service is detected for an IP packet, while the language of the claim provides "monitors whether or not the ~~encryption of~~ information is ~~performed~~ encrypted in accordance with the encryption rule by the information management system on the basis of the process information received over the network from the information management system."

Further, the Office Action relies upon Choo column 9, lines 52-53 and column 10, lines 20-26, which discusses the encrypted or decrypted data passed back to the redirector 509 in the first OS memory area 502 for transmission via a network interface card 505 or routing to an application 504 in case of decryption. However, Choo is silent (there is no evidence of express or inherent disclosure) on any monitoring by the network protocol stack in the first OS memory area 502 in relation to whether data is encrypted by IPsec 510 according to an encryption rule.

The language of claims has a benefit of confirming proper application of an encryption rule, while Choo's IPsec 510 merely checks whether a security service is available and initiates IKE 604 in case the security service is not available.

Further, Choo does not mention the phrase "warning ... the information management system." To establish a prima facie case of anticipation either express or inherent disclosure is required. However, it is readily apparent Choo does not discuss any warning by the IPsec protocol stack 510 to the network protocol stack in the first OS memory area 502. Further, it is readily apparent that Choo could not provide any **warning "over the network."** Further, the Office Action does not provide any rationale as to how Choo inherently or necessarily requires the IPsec protocol stack 510 to give a warning to the network protocol stack in the first OS memory area 502, if a security association is not detected. Further, IKE 604 negotiation is not a warning to anything. Further, Choo is silent (there is no evidence of express or inherent disclosure) on any monitoring by the network protocol stack in the first OS memory area 502 in relation to whether data is encrypted by IPsec 510 according to an encryption rule.

Withdrawal of the rejection of independent claim 1 and allowance of claim 1 is requested. Independent claims 5, 6, 8, 9, and 11 recite limitations similar to independent claim 1 and are allowable.

DEPENDENT CLAIM 2

For example, dependent claim 2 is allowable by claiming a scenario when an encryption rule is changed, namely "***if the cryptography of the encryption system that is indicated in the rule information is changed*, the encryption data transmitting portion ***transmits the encryption data for performing encryption in accordance with the changed encryption system-cryptography to the information management system***, and the warning portion ***warns the information management system to encrypt the perform encryption of information in accordance with the changed encryption-system cryptography***." Allowance of dependent claim 2 is requested.**

Other dependent claims recite patentably distinguishing features of their own or are at least patentably distinguishing due to their dependencies from the independent claims.

CONCLUSION

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,
STAAS & HALSEY LLP

/Mehdi D. Sheikerz/

Date: ____November 29, 2008____ By: _____
Mehdi D. Sheikerz
Registration No. 41,307

1201 New York Avenue, N.W., 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501